

4

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on May 23, 2002.

Clara Magallón

PRELIMINARY AMENDMENT

Post Office Box 7068
Pasadena, CA 91109-7068
May 23, 2002

Before examination please amend the above-identified application as follows:

Before the paragraph beginning at Page 63, Line 31, please insert the following paragraph:

-1-

Docket No. 47187/RRT/S850

message was not tampered with. It verifies that the challenge received is the challenge sent. It verifies that the host's registers are the same as the local data of registers. These above two steps authenticate the host to the PSD as shown by 500E in FIG. 5. The client software signs the challenge that the PSD sent, and also the local record of the customer's ascending and descending registers. It then sends this to the PSD. It sends cleartext of the challenge and the transaction message and sends an HMAC of all of the above, using the shared HMK as shown by 500C. The PSD performs the transaction as shown by 500F.

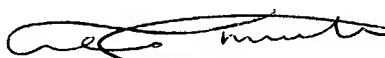
REMARKS

The Initial Patent Examination Division has objected to Applicants' drawings as not being in compliance with 37 CFR §1.84 because they contain excessive text, specifically FIG. 5. Applicant has amended FIG. 5 to comply with 37 CFR §1.84 by removing the excessive text. The Specification is amended to include the removed text. No new matter is added. Attached hereto is a marked-up version of the changes made to the specification by the current amendment. The attached page is captioned "**Version with markings to show changes made.**"

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By


Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/cam

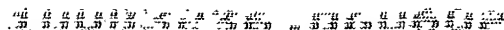
Docket No. 47187/RRT/S850

VERSION WITH MARKINGS TO SHOW CHANGES MADE

The following new paragraph has been inserted before the paragraph beginning at page 63, line 31:

In one embodiment, the client software generates a random 64-bit challenge as shown by 500A in FIG. 5. The PSD signs the host's challenge, using the HMK shared during registration. The PSD returns the above, as well as its own 64-bit challenge as shown by 500D in FIG. 5. The client software compares the HMAC of the challenge it sent with the HMAC it receives from the PSD. The host trusts the PSD for this transaction. The host retains the PSD's challenge to authenticate itself to the PSD as shown by 500B. This ensures that the message was not tampered with. It verifies that the challenge received is the challenge sent. It verifies that the host's registers are the same as the local data of registers. These above two steps authenticate the host to the PSD as shown by 500E in FIG. 5. The client software signs the challenge that the PSD sent, and also the local record of the customer's ascending and descending registers. It then sends this to the PSD. It sends cleartext of the challenge and the transaction message and sends an HMAC of all of the above, using the shared HMK as shown by 500C. The PSD performs the transaction as shown by 500F.

CAM PAS437023.1*-5/23/02 2.10 PM



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Clara Magallón

Applicant	:	Craig L. Ogg, et al.
Application No.	:	10/083,236
Filed	:	February 26, 2002
Title	:	SECURED CENTRALIZED PUBLIC KEY INFRASTRUCTURE
Grp./Div.	:	2132
Examiner	:	Not yet assigned
Docket No.	:	47187/RRT/S850


REQUEST FOR APPROVAL OF AMENDED FIGURES

Post Office Box 7068
Pasadena, CA 91109-7068
May 23, 2002

Commissioner:

Enclosed is corrected FIG. 5, and a marked up red-lined version of FIG. 5 for this application.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By 
Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/cam
Enclosures
CAM PAS437087.1-* -5/23/02 5:05 PM

FIG. 5

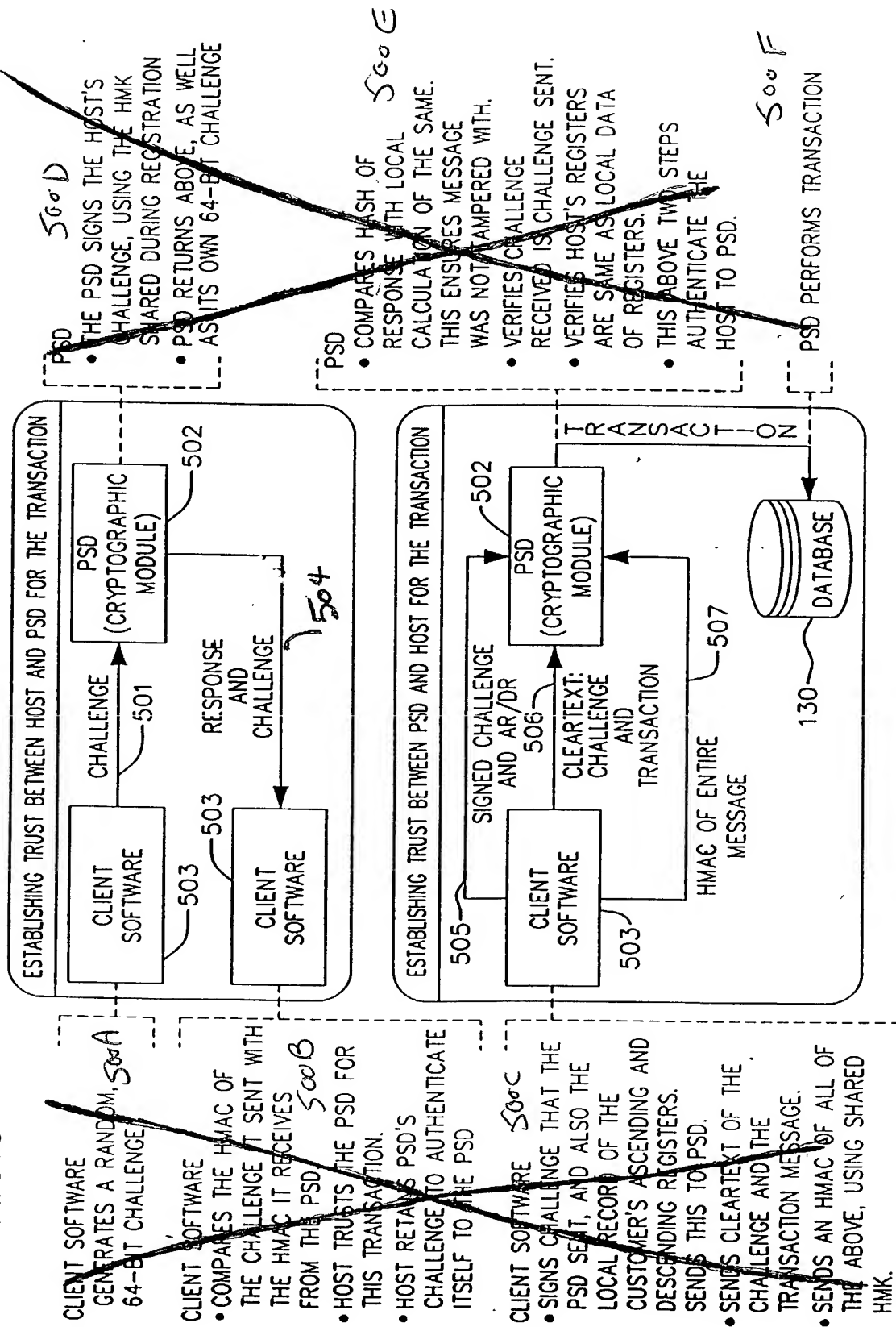


FIG. 5

